ARUBA

ArubaOS

WLAN Switch Software

2.4.1.0 Release Notes

What's New in Release 2.4.1.0

These release notes describe new features in ArubaOS 2.4.1.0 including:

- Remote AP (RAP) now supports local traffic bridging at remote location
- SNMP MIB now supports CPU and memory utilization
- ARM enhancement support for neighbor AP awareness
- Configurable Access Point (AP) Ethernet port speed

These enhancements have the following characteristics:

Remote AP Support for Local Bridging

Enhancements to Remote AP functionality now enables support for local bridging of traffic, allowing WLAN users at the remote location to access resources residing on a local subnet (for example a local print queue or storage server) to be accessed directly without the need to traverse the WAN tunnel back to the central mobility controller. Additionally, this allows non enterprise traffic (Guest access or internet connectivity) to be bridged directly to a subnet bound for the public internet / network. (Note that local bridging features require that you first obtain and install the Remote Access Point license).

SNMP Enhancements

SNMP MIB enhancements now allows administrative users better monitoring capability / visibility into mobility controller CPU and memory utilization levels and system loading.

Neighbor Aware ARM Enhancements

Neighbor aware ARM provides enhanced AP radio channel allocation and management, optimizing the allocation of channels between APs that are unable to directly hear each other, minimizing interference and enhancing RF environment resilience.

Configurable AP Port Speed

This release supports better control over Access Point Ethernet link speed to administrative users, enabling manual configuration of the AP's wired Ethernet port speed and duplex settings to 10/100/Half/Full or Auto. This capability is available from the CLI only and does not support the AP52 or the Aruba 2E. (The CLI command for this feature has been added to the **ap location x.y.z phy-type enet***n* command.

Issues and Limitations Fixed in this Release

The following issues and limitations from 2.4.0.0 have been fixed in this release:

Authentication

- The user entry created on the Home Agent (HA) does not display the correct Location, Roaming, ESSID/BSSID/Phy values. However, this is a display-only issue and the correct values are being enforced. (6151)
- If trim-fqdn is enabled for 802.1x server, the domainname portion for the FQDN is still passed to the RADIUS server by the client internal EAP module. (6898)
- The management authentication default role no longer displays as guest in the CLI but as root in the WebUI. (8161)
- The show station table output is no longer empty when there are a large number of entries. (8266)
- Wired 802.1x no longer fails to authenticate users when mobility is enabled and a role-based VLAN is configured. (8508)

CLI

- Database synchronization no longer fails with a small timeout value when the database size is large. (8251)

Certificate

- When uploading a certificate while using a non-supported browser, you will no longer receive a message that the **`document contains no data`**. However, Aruba recommends that you only use Internet Explorer as your browser. (7928)

Licensing

- When a license key is installed, the system will inform the user that a reboot is necessary to enable the feature associated with the key. The license table now shows that a reboot is required by marking the installed key with an **R** flag. (7845)

Platform

- APs are now consistently deleted from the show ap registered list. (7983)
- Active AP now shows coverage on its floor. (8024)
- The Aruba Wired 2E enet 1 tunnel is now being added to the new VLAN upon changing the native VLAN configuration of enet1 in trunk mode. (7977)

- WEP/TKIP traffic no longer experiences memory contention issues and thus no longer freezes up. (6842)

SNMP

- A trap is now generated when the switch role is changed. (8262)

Soft AP

- The problem with in-band destined traffic occasionally being routed through the out-of-band (mgmt) interface has been fixed. (6629)
- The max-client limit is no longer being ignored. (8218)
- The Network Summary now correctly reports AP status. (8117).
- AP 60s no longer stop sending beacons while configuring virtual APs. (7972)

VPN

- Switches are now able to handle more than 100 PPTP connection requests.(7997)

xSec

- The xSec client is now assigned the correct role as configured in 802.1x. (8175)
- 2.4.0.0 users were able to configure an xSec client on the same VLAN as the AP this client associated with, (which while permitted was not recommended). This is not allowed in 2.4.1.0. Configuring xSec clients on the same VLAN as the associated AP now results in the xSec client not receiving an IP address as the mobility controller does not communicate with the client using xSec if the client is on the same VLAN as the AP.

Known Issues and Limitations in this Release

The following features and functionality have the following issues for Release 2.4.1.0. Where bug IDs are applicable, they are included in the description of the issue.

- If a line card is removed and the switch is rebooted before the line card is replaced, the VLAN configuration reverts to default values. (6226)
- Enabling NAT for source addresses on Aruba switches is compatible with Nortel VPN clients provided a rule is added before the src-nat rule. To support RSA token and time syncing, specify a rule on the client firewall.
- Access Points that are indirectly connected to Aruba Mobility Controllers through third-party switches may have problems processing IP packets larger than 1500 bytes. Aruba recommends setting the maximum transmission unit

(MTU) on these Access Points to 1500 bytes. Do this by entering (from enable mode) under the AP location:

ap location 0.0.0 mtu 1500
write memory

- Aruba only supports directly connecting Aruba Mobility Controllers with a cross-over cable. Connecting Aruba Mobility Controllers with straight-through cables is not recommended. Using the proper (cross-over) cable, ports on both sides of the connection can be configured to auto-negotiate or can be hard coded as long as they match.
- If after upgrading from ArubaOS 2.0.x to 2.4.1.0, you notice that some Ethernet ports fail to come up, check the port setting. It is likely these ports are configured as 100/10 half or full duplex when they should be set to auto-negotiate. (The port configuration mechanism for 2.4.1.0 differs from that in 2.0.x which may cause occasional port misconfigurations.)
- Devices that are idle for extended periods of time (for example, overnight) but which need to maintain their connection to an Aruba switch, must be able to respond to ICMP requests from the Aruba switch. However, the default settings of many personal firewalls, (including XP SP2), deny incoming ICMP requests. This configuration results in the devices experiencing frequent disconnects and reconnects, as well as DHCP address problems. To eliminate connection problems, be sure to configure firewall settings to allow ICMP requests from the Aruba switch.
- Many personal firewalls and ad/pop-up blocker programs, (for example Google and Yahoo) block pop-up windows by default. This can cause Captive Portal logon/logout issues if the switch URL does not explicitly allow pop ups. To prevent this problem, allow pop ups for the switch's URL.
  To log-out from a Captive Portal session if the pop-up window is not available, point your web browser to:

  http://<switch ip address>/auth/logout.html

- In deployments with the Aruba dialer and RSA SecurID, new/next pin mode RSA token time syncing support requires that the Aruba dialer be added into the firewall's application exception list. (For more information on configuring a firewall application exception list, refer to the Microsoft knowledge base, as this is typical for Microsoft applications.) This step is not required for normal operations.
- The Microsoft XP SP2 personal firewall already allows L2TP whereas Sygate needs this to be configured manually.
- RF Plan is a view-only application in MAC OS.
- User entries showing wrong Location and Roaming Status may occur after a failover and recovery. The HA shows the correct information but the FA may not. (6858)

- While moving a station, if 802.1x authentication is delayed, the **show user global-user-map** command output is not displayed correctly. (6557)
- Wired clients who fail authentication are blacklisted, but they can still try to login. (6802)
- Session mirroring does not update for sessions that are already up. (6829)
- All PPTP connections to Aruba (or any PPTP server) for users with Windows XP Service Pack 2 firewall enabled, will experience a one minute wait before being able to reconnect.
- If the username is in the format of domain\username, trim-fqdn does not remove the domain portion before sending request to the server. (6804)
- There is a BW contract granularity limitation. The effective bandwidth enforced is not accurate for contracts less than 300 Kbits. (6838)
- The wired-dot1x role-based VLAN is not supported for SecureJack. (7464)
- WiFiMUX wired 802.1x is not supported in this release. (6310)
- Changes in the NTP Servers list on master switches are not being propagated to local switches. (4944)
- If you are not doing any backend or local database authentication for administrative users, Aruba recommends that you disable this feature by using the **aaa mgmt-authentication mode disable** command.
- To restore the correct syslog facility level from a saved configuration file, do a **write erase** before executing a **copy flash: <saved-cfg> flash: default.cfg**.
- ESI can be used within a multi-switch topology with master and local switches and full redundancy. However, the following limitations apply in this release.

    1. On the WebUI, using the **Back** button to move back to previous browser pages occasionally causes incorrect data, (blanks) to be filled in some fields. This can result in ESI misconfigurations being sent to the switch. (7618).
    2. By design, in a multi-switch topology, client VLANs should not be shared across switches. For example, client VLAN 100 cannot be configured on switch lms1 and lms2 as doing so would cause the AVF routes to be incorrect when the client moves between the switches. Use separate VLANs instead on each switch and let mobility take care of preserving the IP addresses of the client when the client moves between switches.
    3. By design, multi-switch topology will only work in route mode. Bridge mode requires the AVF servers to be directly connected to the Aruba switch as server up/down status is detected by the port link status.
    4. In redundant switch configurations, do not use bridge mode. Use route mode to keep redirected packets properly forwarded. (7912)

- After a role-based VLAN is disabled, the 802.1x client will not have connectivity for a few minutes. (7892)
- Monitoring > Switch Summary may not display the correct total of clients and switches. The WLAN client summary may be smaller than the total of client entries because the per-switch display includes additional entries – which are not shown in the global user list. (7904)
- When you upload a license certificate, fpweb will restart. This is normal. However, the restart event is incorrectly logged as an fpweb crash. You can ignore this log message. (7940)
- After restoring a configuration, verify that your logging levels are set properly as they may not be restored. (7542)
- If you have licensed features on a Supervisor Card and need to replace that card, be sure to restore the configuration from backup on the new card to restore your license information. For more information, refer to the Managing Software Feature Licenses document that ships with your switch.
- Using A60/61 APs with Cisco 3550 PoE switches requires the Cisco switches to running IOS 12.1 (19) or later. Aruba recommends that you also make the following configuration settings on the Cisco 3550 (INLINE POWER) port:
    - power inline delay shutdown 15 initial 25
    - (config-if) spanning-tree portfast
- The 800-E and the 2400-E Gigethernet ports only support 1000Base-T rates.
- In this release, if the logging level of authmgr (formerly known as arubaauth) is set to a non-default level, when the Switch is upgraded to 2.4, the logging level is changed to the default level of Informational. (7959)
- Sygate SODA users should note that upload file names cannot contain spaces.
- Wired clients appear on All WLAN Clients pages in the WebUI .(7968)
- Funk-Odyssey clients may experience delays in getting authenticated when using WPA encryption and server derivation roles where the VLAN of the client is set by matching a particular attribute. Aruba recommends that these users set the WPA Key Timeout and WPA Retry Count to 5.
- Due to current limitations in the Funk-Odyssey client software, clients cannot associate via a third-party APs or Bridges if xSec encryption is selected. (7684)
- xSec cannot be enabled on uplink trunk ports doing dot1q tagging. (7704)
- Some client NICs (for example, Dlink, 3Com) may experience problems sending frames when the MTU size exceeds 1408 bytes (7963)
- The message: “Please reload the switch for the new service key to take effect” continues to display even after an existing temporary key is replaced with another temporary or permanent key. A reboot is not required if the associated feature is already enabled (as shown by the show keys CLI command or on the WebUI license management page). (7214)
- The message: “Reboot Cause: License Expired” displays with the **show switchinfo** CLI command output, but does not specify which of the licenses has expired and caused a scheduled system reboot. (7215)

- No SNMP traps are generated when software feature licenses are added, deleted, or expire. Syslog messages, however do report these events.(7450)
- Sygate SMS does not return MPPE keys when user authentication fails and host authentication is passed. (7736)
- When Sygate Virtual Desktop check is enabled, the first check will always fails and the subsequent check will pass. (7501)
- When switches are configured for ESI in bridge mode, and an ARP entry for the gateway does not exist (for example, during switch boot up or just after a clear ARP command), the switch will not redirect packets to the destination. To fix this problem, either enter a static ARP entry for the default gateway or ping the default gateway to create an ARP entry. (8016)
- When using some legacy Cisco Access Points (for example the Cisco AP 1200), be aware of the following condition when using PoE:
  - The Cisco AP is connected to an Aruba mobility controller.
  - Cisco mode is enabled (**poe cisco**).
  - PoE is turned off (**no poe**).
  - PoE is turned back on (**poe**).
  - Cisco mode is re-enabled (**poe cisco**)

  The Cisco AP does not power on. To resolve this condition, enter **no poe cisco**. The Cisco AP will now function normally as a PoE device. (8054, 7442)
- The multicast key often fails to install for low performance CPUs like FOMA N900iL. (8171)
- When deleting large blocks of users, they are removed from the user list as well as mobile client list but user global list still shows the user entries with a zero IP address value (7960)
- The Captive Portal Login page is not configurable in the WebUI. (8135)
- No accounting record is sent out after a BOAP user authenticates. (8093)
- A command is needed to find out the encryption/decryption statistics from the AP. (8072)
- User entries in globalTable do not agree with user entries on the switch. (8264)
- Occasionally, moving a user from HA to FA and back to HA causes the mobile debug future visitor table to display incorrectly. (7589)
- Changing an AP name in RF plan is only temporary. (7293)
- Some Access Points are displayed twice with status as up for one and down for the other. (8128).
- LDAP servers with base-dn configured with an empty string report an error in IE. (8181).
- Incorrect tunnel location is displayed by show user command for mux clients. (8202)
- Bandwidth for the Aruba 2E is limited and shared in duplex mode. (7397)
- 10M half-duplex traffic on enet 0 for the Aruba 2E has low throughput. (7400)
- Unable to place more than 5 phone conversations using wpa2-aes-psk. (8102)

- Occasionally the SNMP community does not appear in the WebUI until the page is refreshed. (7867)
- On the WebUI, navigating to AP >Status > Client may produce an error. (8285)
- Occasionally, when all the parameters are configured in the LDAP server page of the WebUI, only some of the configured parameters are applied. (8023)
- ESI may report incorrect servers in the datapath when servers were moved around within a group. (7792)
- Some 2Es may report one of the 2E ports as a user on the local switch. (7365)
- The **Monitoring** > **Switch** > **Access Points Status** and **Profile** buttons properly display AP data only for APs on the first page. If you have more APs than will display on the first page, AP data does not display properly when you click **Status** or **Profile** on these pages. The APs appear, but when you click **Status**, no AP status data appears. When you click **Profile**, only partial AP profile data appears.)
  For switches supporting less than 100 APs, you can increase the maximum page size (up to 100, which is the upper limit) to keep all the APs on one page. Otherwise, be advised that displays on subsequent pages will be incomplete.
- When Offline RF Plan is newly installed on a Windows XP-SP2 machine, the error message: Can't create XMLHttpRequest object: Automation server can't create object" may appear. You can ignore this message. (7965)
- 802.1x role-based VLAN derivation is not working for xSec clients. (8304)
- Access Multiplexer (800-E and 2400-E) 802.1x users are not able to reconnect if the disconnect and reconnect intervals are too short (less than ten seconds). (8238)
- Do not enable stateful and wired 802.1x authentication methods at the same time. If either one is enabled, make sure the other is disabled (8289)
- The "A" channel in ARM configurations has been observed in one installation to change channels frequently. It is not clear if this problem is related to the site or to the version of ArubaOS being run, but this bug has not been observed in the lab with the current software and further testing is required. (7108)
- When users select a port in the ports page of the WebUI, select trunk port, and click **Apply**, the following error message appears:
  Configuration Failed: Port Configuration is not Changed :: Interface is a Trunk port. This message can be ignored as the configuration is changed correctly. (8520)

Upgrading or Downgrading

If the software upgrade distributed with these release notes is on CD or some other static media, be sure to go to the Customer Support website to make sure you have the latest release of ArubaOS.

For information on upgrading to, or downgrading from, 2.4.1.0, refer to Installing ArubaOS 2.4.1.0—Prerequisites.

Before you Change your Switch’s Image

All Aruba Mobility Controllers store critical configuration data on an onboard Compact Flash memory module. In order to maintain the reliability of your Aruba WLAN network, Aruba recommends the following general best practices with respect to the use of your Aruba switch and its Compact Flash memory:

Backing up Critical Data

It is important to back up frequently all critical configuration data and files on Compact Flash file system to an off-switch external server or mass storage facility. At the very least, you should include the following files in these frequent off-switch backups:

- Configuration Data
- WMS Database
- Local User Database
- Licensing Database
- Floor Plan JPEGs
- Customer Captive Portal Pages
- Customer x.509 Certificates

Managing Flash Memory

Be careful not to exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan can consume the flash space quickly. Warning messages will alert you that the file system is running out of space whenever any write attempt to Flash occurs once there is 5Mbytes or less of space remaining.

Other tasks which are sensitive to insufficient Flash file system space include:

- Using the internal database - DHCP lease/renew information etc. is also stored on Flash. If the file system is full, DHCP addresses will not be distributed/renewed.

- If an Aruba switch encounters a bug where it needs to write a core file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost.

Powering the System Down or Power Cycling the System

Compact Flash devices can be corrupted if power is lost during a write event (for example. **write mem**). To reduce the exposure of Compact Flash to corruption, be sure to follow these procedures:

For AirOS release 2.2 or greater:

- To power down:
  - From the CLI, type: **halt**.
  - The switch will respond with the message: **system halted**.
  - Now the switch is ready to be powered down or reset (at this point will automatically reset after approximately 90 seconds).

For releases prior to AirOS 2.2:

- To power down:
  - From the CLI type **reload**
  - Linux will shut down and when you see **Hit any key to stop autoboot**: message, press Enter.
  - You are now at the cpboot prompt (cpboot>) and the switch is ready to be powered down or reset.

Installing ArubaOS 2.4.1.0—Prerequisites

- Make sure you have at least 10MB free flash.
- Back up the WMS database and TFTP it off the switch.
- Remove all unnecessary saved files from flash.
- Run the tar crash command to make sure that there are no "process died" files clogging up memory and TFTP the files off the switch.

Upgrading to ArubaOS 2.4.1.0

The Aruba ArubaOS software can be upgraded as new releases become available. The following steps abbreviate the detailed procedures located in the *Aruba ArubaOS 2.4 User’s Guide*.

Caution — When upgrading the software in a multi-switch network (one that uses two or more Aruba Mobility Controllers), special care must be taken to upgrade all the Mobility Controllers in the network and to upgrade them in the proper sequence (see Upgrading Multi-Switch Networks

1 Obtain the latest, valid Aruba Mobility Controller software image from Aruba Customer Support.

Note— The most current Aruba Mobility Controller software image may be newer than that available at the time these release notes were written. Aruba recommends that you always download the latest software image from Aruba Customer Support before proceeding with these installation instructions.

2 Upload the new software image to a TFTP server on your network.

3 Verify the network connection between from the target switch to the TFTP server:

```
(aruba) # ping <TFTP server IP address>
```

4 Backup your current switch configuration.

Use the following command to determine the name of your configuration file:

```
(aruba) # show boot
Config File: default.cfg
Boot Partition: PARTITION 0
```

In this example, `default.cfg` is the configuration filename. To copy the configuration file to an external TFTP server, use the following command:

```
(aruba) # copy flash: default.cfg tftp: <TFTP server IP address> <dest. filename>
```

Note— A valid IP route must exist between the TFTP server and the Mobility Controller. Also required, a placeholder file with the destination filename and proper write permissions must exist on the TFTP server prior to executing the copy command.

5 Backup your current WMS and local user databases.

Use the following commands to export the Mobility Controller’s internal databases to an internal file with the filename of your choice, and then to an external TFTP server:

```
(aruba) # wms export-db <filename for WMS db>
(aruba) # copy flash: <filename for db> tftp: <TFTP server IP address> <dest. filename>
(aruba) # local-userdb export <filename for local user db>
(aruba) # copy flash: <filename for db> tftp: <TFTP server IP address> <dest. filename>
```

Note— A valid IP route must exist between the TFTP server and the Mobility Controller. Also required, a placeholder file with the proper write permissions for each destination filename must exist on the TFTP server prior to executing the copy commands.

6 Determine which memory partition will be used to hold the new software image.

Use the following command to check the memory partitions:

```
(aruba) # show image version
----------------------------------
Partition                : 0:0 (/dev/hda1) **Default boot**
Software Version         : 2.4.1.0
Build number             : 10682
Built on                 : Mon Jun 27 05:52:19 PDT 2005
----------------------------------
Partition                : 0:1 (/dev/hda2)
/dev/hda2: Image not present
----------------------------------
Partition                : 1:0 (/dev/hdc1)
Not plugged in.
----------------------------------
Partition                : 1:1 (/dev/hdc2)
Not plugged in.
```

It is recommended to load the new image into the backup partition. In the above example, partition 0 contains the active image. Partition 1 is empty (`image not present`) and can be used for loading the new software.

7 Use the **copy** command to load the new image into the Aruba Mobility Controller:

# **copy tftp:** <*server address*> <*image filename*> **system: partition** {**0**|**1**}

Note— When using the copy command to load a software image, the specified partition automatically becomes active the next time the switch is rebooted. There is no need manually select the partition.

8 Verify that the new image is loaded:

# **show image version**

Information about the newly loaded software image should be displayed for the appropriate partition.

9 Reboot the switch:

```
# reload
```

10 When the boot process is complete, use the **show version** command to verify the upgrade.

```
(Aruba) #show version
Aruba Operating System Software.
ArubaOS (MODEL: Aruba800), Version 2.4.1.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2005, Aruba Wireless Networks Inc.
Compiled on 2005-06-27 at 17:25:38 PDT (build 10682) by p4build

ROM: System Bootstrap, Version CPBoot 1.2.9 (Mar 11 2005 - 16:04:02)

Switch uptime is 22 minutes 42 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor (revision 16.20 (pvr 8081 1014)) with 256M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=SMART ATA FLASH).

(aruba) #
```

In this example, version 2.4.1.0 is loaded and running, indicating that the upgrade is complete.

11 Log in as the administrator and set the proper time zone for your location.

(config) # **clock timezone** *<name of timezone>* *<UTC offset>*

Upgrading Multi-Switch Networks

In a multi-switch network (one with two or more Mobility Controllers), special care must be taken to upgrade all switches in the proper sequence, based on the switch type (master or local). Be sure to back up all switches being upgraded.

1. Make sure you have at least 10MB free flash.
2. Back up the WMS database and TFTP it off the switch.
3. Remove all unnecessary saved files from flash.
4. Run the tar crash command to make sure that there are no "process died" files clogging up memory and TFTP the files off the switch.

Upgrading to ArubaOS 2.4.1.0

Upgrading an Existing Network

To upgrade an existing multi-switch system to ArubaOS 2.4.1.0:

1. Upgrade the master Mobility Controller first.
2. Upgrade all local Mobility Controllers last.

Note— For proper operation, all Mobility Controllers in the network must be upgraded to use the same version of ArubaOS software.

Upgrading Redundant Switches

When configuring master/local switches in a redundant (VRRP) environment, the redundant switches should be the same class of switch (5000, 2400, or 800) or better, running the same revision of ArubaOS.

1. Aruba recommends upgrading in the following order:
2. Upgrade the Master switch to the new code.
3. Reboot the Master switch.

4. Upgrade the Local switches to the new code.

5. Do not reboot the Local switches yet.

6. From the Master CLI, enter
   `apboot location 0.0.0`

7. Now reboot the Local switches.

The APs should now have the new version of ArubaOS since they were rebooted and not failed over through VRRP.

Reverting to AirOS 2.X.X.X

If necessary, you can to return to your previous version of AirOS 2.X.X.X software after upgrading to a newer version. Be sure to back up your switch before reverting the OS. Also import the local database and the WMS database.

Caution — When reverting the Mobility Controller software, whenever possible use the previous version of software known to be used on the system. Loading a different prior release not specifically confirmed to operate in your environment could result in an improper configuration.

1. Determine the name of the current configuration file.

```
(aruba) #show boot
Config File: default.cfg


Boot Partition: PARTITION 1
```

In this example, `default.cfg` is the name of the configuration file.

2. Determine where your backup software is stored.

   Use the following command to check the memory partitions:

```
(aruba) #show image ver
----------------------------------
Partition                : 0:0 (/dev/hda1)
Software Version         : 2.2.3.0
Build number             : 8096
Label                    : 8096
Built on                 : 2004-07-07 01:26:15 PDT
----------------------------------
Partition                : 0:1 (/dev/hda2) **Default boot**
Software Version         : 2.4.1.0
Build number             : 10682
Label                    : 10682
Built on                 : 2005-6-27 15:02:41 PDT
----------------------------------
Partition                : 1:0 (/dev/hdc1)
Not plugged in.
----------------------------------
Partition                : 1:1 (/dev/hdc2)
Not plugged in.
```

In this example, partition 0, contains the AirOS 2.2.3.0 backup. Partition 1, the active partition, contains the ArubaOS 2.4.1.0 image.

To select the backup partition as the new boot partition:

```
# boot system partition 0
```

3 If you have your backup configuration file on an external TFTP server, use the following command to copy it to the switch:

```
# copy tftp: <TFTP server IP address> <backup filename> flash:
<backup configuration filename>
```

4 Boot to your backup file as you cannot overwrite the active configuration file.

```
# boot config <backup configuration filename>
```

5 Then replace the current configuration file with your backup.

```
# copy flash: <backup configuration filename> flash:
default.cfg
```

6 Boot to your `default.cfg` file.

```
# boot config default.cfg
```

7 Replace the current WMS database file with your backup.

If you have your backup database file on an external TFTP server, use the following commands to import it:

```
# copy tftp: <TFTP server IP address> <backup wms filename>
flash: <wms filename>
```

```
# wms import-db <wmsfilename>
```

If no backup image is present, load one:

```
# copy tftp: <server address> <image filename> system:
partition {0|1}
```

8 Select the backup partition as the new boot partition:

```
# boot system partition {0|1}
```

9 Reboot the switch:

```
# reload
```

10 When the boot process is complete, verify that the switch is using the correct software:

```
# show version
```

Note— When reverting from ArubaOS 2.4.1.0 to AirOS 2.2.3.0 or earlier, all virtual APs that were provisioned in release 2.4.1.0 will have to be reprovisioned.

Troubleshooting

If the switch gets into trouble (for example, insufficient – less than 10MB – flash space), do the following:

1. Disconnect the link to the APs.
2. Remove all unnecessary files from flash, including the db_dump.sql type files.
3. Remove any crash files.
4. Import the old wms DB file and reboot.
5. Reconnect the link for the APs.

Documents in this Release

The following new or revised documents are included in this release:

0500118	Aruba ArubaOS 2.4, User Guide
0500110	Aruba 800-E Wired Access Point Installation Guide
0500111	Aruba 2400-E Wired Access Point Installation Guide

This documentation library is updated continuously. You can download the latest version of any of these documents from:

https://support.arubanetworks.com

For More Information

To contact Aruba Wireless Networks, refer to the information below:

Address

1322 Crossman Avenue

Sunnyvale, CA 94089

Phone

408 227 4500 (main)

408 227 4550 (fax)

Email

info@arubanetworks.com

Website

www.arubanetworks.com

Support

Phone:

US Toll Free: 1 800 WiFiLan (1 800 943 4526)
International: 1 408 754 1200

Email:

support@arubanetworks.com

Website:

http://www.arubanetworks.com/support